

UNITED STATES DISTRICT COURT
Western DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF)
THE PREMISES LOCATED AT: 1310) No. 23-SW-03026-WJE
Swifts HWY, UNIT D205, Jefferson City,)
Missouri 65101 located in the Western) **FILED UNDER SEAL**
District of Missouri.

SIGNED AND SUBMITTED TO THE COURT FOR
FILING BY RELIABLE ELECTRONIC MEANS

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Mark Kutrip, a Special Agent with Homeland Security Investigations, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 1310 Swifts HWY, UNIT D205, Jefferson City, Missouri 65101 which is located in the Western District of Missouri (hereinafter the "SUBJECT PREMISES"), further described in Attachment A, for the things described in Attachment B.

2. I have been employed as a Special Agent ("SA") of the U.S. Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations ("HSI"), since December 2019, and am currently assigned to the HSI office in Saint Louis, Missouri. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center (FLETC) in Brunswick, Georgia, and investigative casework relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and

have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251(a) (production of child pornography), 18 U.S.C. § 2252A(a)(1) and (2) (distribution of child pornography), and 2252A(a)(5)(B) (possession of child pornography) (hereinafter the “SUBJECT OFFENSES”) are presently located at the location to be searched, and within computer(s) and related peripherals, computer hardware and media, and wireless telephones found at that location.

LOCATION TO BE SEARCHED

5. The location to be searched (the “SUBJECT PREMISES”) is located at 1310 SWIFTS HWY, UNIT D205, Jefferson City, Missouri 65101, is a condominium located in the building labeled with the letter D. The building is brick and creme colored. The residence is located on the second floor on the North side of the building. The door of the residence bears the number D205 clearly marked. A photograph of the home is attached to this Affidavit and labeled as “Attachment A”.

6. SUBJECT PREMESIS includes any other outbuildings, structures, vehicles or other storage areas associated with the SUBJECT PREMESIS that may contain, conceal or store evidence, as defined in Attachment B, of the violations outlined within this affidavit.

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment B:
- a. "Cache" refers to text, image and graphic files sent to and temporarily stored by a user's computer from a web site accessed by the user in order to allow the user speedier access to and interaction with that web site.
 - b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.
 - c. "Child pornography," as defined in 18 U.S.C. § 2256(8), includes any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, or the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.
 - d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility

directly related to or operating in conjunction with such device” and includes smartphones and wireless telephones.

- e. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, “thumb,” “jump,” or “flash” drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).
- f. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or

“booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

- g. “Geo-located,” as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.
- h. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.
- i. An “Internet Protocol address” or “IP address,” as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (“ISPs”) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

- j. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- k. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.
- l. “Mobile applications,” as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, sharing photos or videos, reading a book, or playing a game.
- m. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.
- n. “Remote computing service,” as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.
- o. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

- p. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.
- q. The term “web site” consists of text pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol.
- r. “Wireless telephone or mobile telephone, or cellular telephone or cell phone or smartphone” as used herein means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may

have wireless connection capabilities such as Wi-Fi and Bluetooth. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

COMPUTERS AND CHILD PORNOGRAPHY

8. From my own training and experience in the area of Internet-based child exploitation investigations, and through consultation with other knowledgeable law enforcement officials, I know the following to be true. Computers connected to the Internet identify each other by an Internet Protocol (“IP”) address. An IP address can assist law enforcement in finding a particular computer on the Internet. These IP addresses can typically lead a law enforcement officer to a particular Internet service company and that company can typically identify the account that uses or used the address to access the Internet.

9. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed and utilized. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. To distribute these images on any scale also required significant resources. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. More recently, through the use of computers and wireless telephones, child pornography is traded through the Internet, by using, for example, file sharing software.

10. Producers of child pornography can now produce both still and moving images directly from a common video or digital camera, as well as from a wireless telephone. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute

child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow.

11. The Internet allows any computer (including wireless telephone) to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers are sometimes operated by commercial ISPs which allow subscribers to connect to a network which is, in turn, connected to the host systems. Host computers, including ISPs, allow e-mail service between subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web.

12. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography; and (ii) Web sites that offer images of child pornography. Child pornography collectors can use standard Internet connections to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions between child pornography collectors over the Internet. Sometimes the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the recipient's computer, including the Internet history and cache to look for "footprints" of the Web sites and images accessed by the recipient.

PROBABLE CAUSE

13. On or about November 2022, Homeland Security Investigations HSI Cocoa Beach, Florida, HSI Harrisburg, Pennsylvania and HSI Scranton, Pennsylvania initiated an undercover (UC) online investigation involving a subject, known as “DARKRAVEN329” seeking to have sex with the undercover agent’s minor child. During the UC conversation with “DARKRAVEN329” he alleged that he has had some sexual contact with minor children in the past.
14. “DARKRAVEN329” has sent the UC a photograph, and he states his name is Mason. Based on that photograph and the name he provided, through investigative techniques it is believe his name is Mason MOREY.
15. On December 8, 2022, MOREY was arrested in the Middle District of Pennsylvania for violation of 18 U.S.C. 2422(b), attempted online enticement of a minor. On that same date, five (5) cellular telephones were seized from MOREY.
16. On or about December 29, 2022, digital extractions of MOREY’s five (5) cellular telephones were completed by an HSI Computer Forensic Analyst (CFA). Review of the data extracted from the cellular telephones revealed a conversation within the Kik application with an unknown individual using the Kik display name “Fun Forall”, username "fwbfunj". The Kik conversation contained child pornography / child sexual abuse material (CSAM) including videos and images that were self-produced by MOREY.

17. The following is an excerpt of the conversation between MOREY (Cell Phone #02) and Kik display name Fun Forall. This transcript does not detail the full conversation that occurred, but mainly highlights the points needed for the purpose of this affidavit.

a. Saturday, December 3, (2022)

Cell Phone #02: How've you been

Fun Forall: Always so horny

b. Sunday, December 4, (2022)

Fun Forall: I sucked 2 cocks yesterday (This message was sent at 14:04 UTC utilizing IP address 184.97.226.51)

Cell Phone #02: Oh nice bet it was fun time! Wish you were sucking me and my boys too

Fun Forall: Any new pics?

Cell Phone #02: Not yet... would you like me to take some?

Fun Forall: Yes please

Cell Phone #02: What would you like to see?

Fun Forall: You naked of course

Fun Forall: Maybe the boys sitting on your lap

Cell Phone #02: While I'm naked?

Fun Forall: Yes

Cell Phone #02: Might get hard if I do that

Fun Forall: That's ok lol

Cell Phone #02: You'd probably like that wouldn't you

Fun Forall: You know I would (This message was sent at 22:03 UTC utilizing IP address 184.97.226.51)

Fun Forall: Show me lol

Cell Phone #02: I'll have to show you tomorrow morning then

Fun Forall: Why tomorrow morning??

Cell Phone #02: That's when I'll be with them

Fun Forall: Oh

Fun Forall: Are they grabbing it more? (This message was sent at 22:16 UTC utilizing IP address 184.97.226.51)

Cell Phone #02: No, they do tend to look at it more though

c. Monday, December 5, (2022)

Fun Forall: Nice! Can't wait to see this morning (This message was sent at 11:50 UTC utilizing IP address 184.97.226.51)

Cell Phone #02: We'll see if I can do anything right now the youngest is asleep I think he had a cold. And after I pick up the older boy from school I'm not sure if I'll be free to jerk off.

d. Tuesday, December 6, (2022)

Fun Forall: Lol I knew I wouldn't get them

e. Wednesday, December 7, (2022)

Cell Phone #02: How about you see today

Cell Phone #02: I'm already naked and hard

Fun Forall: Are they too?

Cell Phone #02: They are

Cell Phone #02: (sends image #1, image #2, image #3, and video #1 from the cell phone camera)

18. Image #1 was located on cell phone #02 as file name, 4186a2b8-a08d-4f1c-a5ac-831b3a00c295.jpg and has a created date of December 7, 2022, at 11:02:12 AM. Image #1 depicts a toddler aged minor male victim (MMV #1) lying on the floor while on a blanket that is blue and white with blue polka-dots and next to a small giraffe toy. MMV #1 has one (1) eye open and is wearing a green and black striped shirt with black pants. Image #1 also shows an adult male standing over MMV #1 with the adult male displaying his erect penis.
19. Image #2 was located on cell phone #02 as file name, d415b9b0-c6c7-4332-9637-5b02527d5d90.jpg and has a created date of December 7, 2022, at 11:02:35 AM. Image #2 depicts an adult male sitting and displaying his erect penis in front of a minor male victim (MMV #2). The adult male's hand appears to be motioning for MMV #2 to give his hand to the adult male. MMV #2's left hand is shown to be partially open while holding a small toy in the other hand. MMV #2 is wearing a gray t-shirt with black sleeves and the words "oh yeah!" on the front. MMV #2 is also wearing Spiderman pajama pants.
20. Image #3 was located on cell phone #02 as file name, 57b41871-9ecb-4673-b01e-2cc51a9765db.jpg and has a created date of December 7, 2022, at 11:02:44 AM. Image #3 depicts an adult male sitting and displaying his erect penis while MMV #2 is grasping the head of the adult male's erect penis with MMV #2's left hand and MMV #2 is

holding a small toy in his right hand. MMV #2 is wearing a gray t-shirt with black sleeves and the words “oh yeah!” on the front. MMV #2 is also wearing Spiderman pajama pants.

21. Video #1 was located on cell phone #02 as file name, fd204262-bcbf-4f42-9c48-80688649b333.mp4 and has a created date of December 7, 2022, at 11:03:11 AM. Video #1 is 14 seconds in length and depicts MMV #2 using his left hand to rub and squeeze the head of the man’s erect penis. MMV #2 indicates that something is on his finger and wipes his hand on his shirt then continues to grab the man’s erect penis. MMV #2 is holding a small toy in his right hand. MMV #2 is wearing a gray t-shirt with black sleeves and the words “oh yeah!” on the front. MMV #2 is also wearing Spiderman pajama pants.

Fun Forall: Oh he likes it doesn’t he!!

Cell Phone #02: I think he does

Cell Phone #02: Is it turning you on?

Fun Forall: Omg yes!! You must have precum!

Cell Phone #02: (sends video #2 from the cell phone camera)

22. Video #2 was located on cell phone #02 as file name, b34052b1-d9a4-444f-95a7-116a3942a6bc.mp4 and has a created date of December 7, 2022, at 11:04:11 AM. Video #2 is 14 seconds in length and depicts MMV #2 using his fingers from his left hand to hold the head of the adult male’s erect penis while moving the adult male’s penis in a back-and-forth/ side -to -side motion. MMV #2 is holding a toy with his right hand.

MMV #2 is wearing a gray t-shirt with black sleeves and the words “oh yeah!” on the front. MMV #2 is also wearing spiderman pajama pants.

Fun Forall: He probably wants to taste it!!

Cell Phone #02: Oh maybe he will

Fun Forall: Does his hand feel good??

Cell Phone #02: What would you do if you were here?

Cell Phone #02: yes it feels so great

Fun Forall: I’d let him feel me too!

Fun Forall: I’d feel his too! Is he hard?

Cell Phone #02: He’s not hard yet

Fun Forall: He might need help

Cell Phone #02: Think I should help him out?

Fun Forall: Definitely!!

Fun Forall: Can I see?

Cell Phone #02: If I can see you?

Fun Forall: I’m at work, nothing good to show rn lol (sends image #1a)

23. Image #1a is a black and white photograph of a white female with light colored eyes. The specific color of the eyes is unable to be determined due to the photograph being in black and white. The female has light colored hair and a stud nose piercing in her right nostril.

Cell Phone #02: Maybe you’ll show more later? Very beautiful

Fun Forall: I wish I was naked and playing with myself

Fun Forall: Or he could watch me blowing you if I was there

Cell Phone #02: I want you to touch yourself later thinking of my boys and I

Cell Phone #02: You could teach him how to suck properly

Fun Forall: OMG yes!!

Fun Forall: You should help him now though

Cell Phone #02: (sends image #4 from the cell phone camera)

24. Image #4 was located on cell phone #02 as file name, c6bff5e0-9cb1-43bb-bd40-84fdda1287a1.jpg and has a created date of December 7, 2022, at 11:14:42 AM. Image #4 depicts an adult male sitting and displaying his erect penis while grabbing hold of MMV #2 by MMV #2's gray t-shirt. MMV #2 is standing between the adult male's legs and MMV #2 is undressed from the waist down with MMV #2's penis made visible in the center of the image.

Fun Forall: Show me you getting him hard please!

Cell Phone #02: (sends image #5 and video #3 from the cell phone camera)

25. Image #5 was located on cell phone #02 as file name, c14f9789-ea3e-423f-9a49-360b64344904.jpg and has a created date of December 7, 2022, at 11:17:47 AM. Image #5 depicts an adult male sitting and displaying his erect penis while MMV #2 is sitting on the adult male's lap with MMV #2's genitalia displayed next to the adult male's penis.
26. Video #3 was located on cell phone #02 as file name, dff63b9e-3e67-4748-a511-6c727ac5f3ba.mp4 and has a created date of December 7, 2022, at 11:18:09 AM. Video #3 is 14 seconds in length and depicts what appears to be the fingers of an adult male holding and manually stimulating MMV #2's penis.

Fun Forall: He's thick!

27. Cell Phone #02: (sends image #6 and image #7 from the cell phone camera)
28. Image #6 was located on cell phone #02 as file name, 0383ff9d-f842-4b7a-af7b-1b418c2eb1bb.jpg and has a created date of December 7, 2022, at 11:18:28 AM. Image #6 depicts MMV #2 with an erect penis and sitting on an adult male's lap. The adult male is grasping both his erect penis and MMV #2's erect penis together with the adult male's left hand.
29. Image #7 was located on cell phone #02 as file name, 2a1da3dd-e7d9-4ad7-86a2-731f758703b1.jpg and has a created date of December 7, 2022, at 11:18:46 AM. Image #7 depicts MMV #2 holding his penis with his own right hand. An adult male's erect penis is visible under MMV #2's leg.

Fun Forall: Is he liking it?

Cell Phone #02: He definitely

Cell Phone #02: (send video #4 from the cell phone camera)

30. Video #4 was located on cell phone #02 as file name, 3a2d2a82-bd5f-4dc5-8efc-5f695a57bd5b.mp4 and has a created date of December 7, 2022, at 11:19:09 AM. Video #4 is 6 seconds in length and depicts MMV #2 stimulating his own erect penis while sitting on an adult male's lap. The adult male's erect penis is displayed between MMV #2's legs.

Fun Forall: Omg I'd suck you both!!

Fun Forall: I bet you're going to cum so hard!!

Fun Forall: Are you going to cum on him?

Cell Phone #02: (sends video #5 from the cell phone camera)

31. Video #5 was located on cell phone #02 as file name, 7ba5f891-3fe7-42c4-9b3d-b662b169cc4f.mp4 and has a created date of December 7, 2022, at 11:21:01 AM. Video #5 is 14 seconds in length and depicts what appears to be an adult male's left hand grasping both his own erect penis and MMV #2's erect penis together while manually stimulating both.

Cell Phone #02: Oh yeah I'm definitely getting ready to cum

Fun Forall: Show him how Dad cums on his cock!

Cell Phone #02: (sends video #6 from the cell phone camera)

32. Video #6 was located on cell phone #02 as file name, a51fdc40-6332-4d20-8e74-f10cd33d5a6e.mp4 and has a created date of December 7, 2022, at 11:22:23 AM. Video #6 is 11 seconds in length and depicts what appears to be an adult male's left hand grasping both his erect penis and MMV #2's erect penis together while manually stimulating both. The adult male then ejaculates on himself and on MMV #2.

Fun Forall: Omg you came so much!! He want to feel your cum didn't he!! Did he taste it?

Cell Phone #02: Yeah I did lol and he definitely felt it I don't think he likes it he tried wiping it off right away..

Fun Forall: I bet he'll want to do it more

Cell Phone #02: He might!

Cell Phone #02: He was definitely liking playing with it

Cell Phone #02: Are you going to play with yourself when you get home while watching the videos?

Fun Forall: Omg yes

Fun Forall: Was your other son watching you

Cell Phone #02: he wasn't. He was watching tv

Fun Forall: Lol he's still a little young

Fun Forall: Your older one was definitely having fun

Cell Phone #02: He'll get there too though

Cell Phone #02: Maybe someday he'll want to taste my dick rather than just hold it

Fun Forall: Rub some candy on it first lol

Cell Phone #02: Or you could show him how it's done so he copies you

Fun Forall: Oh I definitely would!!

Cell Phone #02: Where are you from again?

Cell Phone #02: And he can watch me fucking you too and learn how to go inside you

Fun Forall: Missouri, you?

Fun Forall: I'd let him learn everything from us!

Cell Phone #02: Pennsylvania. Maybe you should come up and visit sometime

Fun Forall: Where in Pennsylvania?

Cell Phone #02: Lebanon

Fun Forall: Do you have full time custody or share with their mom

Cell Phone #02: Well at this point they live totally with their mom. I'm at her place watching them during the day.

Fun Forall: ooohhhh so she's at work?

Cell Phone #02: yep

Cell Phone #02: You could always stay at a hotel and come visit during the day

Fun Forall: That's probably beyond my budget lol

Cell Phone #02: Who said I wouldn't pay for you?

Fun Forall: Is rather you use it to get your own place

Cell Phone #02: I'll definitely have to do that soon and have you over

Fun Forall: Yes please!!

Cell Phone #02: What would you wear while you were here?

Fun Forall: Would I have to wear anything?

Cell Phone #02: No, that would be better not to

Fun Forall: That's what I was thinking

Cell Phone #02: Good way to think

The conversation ended.

33. On January 27, 2023, HSI and Pennsylvania State Police (PSP) Agents were able to positively identify MMV #1 and MMV #2. HSI and PSP Agents also identified and photographed some of the clothing and items that were shown in Image #1, Image #2, Image #3, Image #4, Video #1, and Video #2.

34. On February 15, 2023, a subpoena was sent to Kik for the subscriber information related to the display name "Fun Forall"/username "fwbfunjc". Subpoena request number KIK-11701. Kik provided subscriber information for Kik username fwbfunjc.

First Name: Fun

Last Name: Forall

Email: fwbfunj@gmail.com

Username: fwbfunj

35. Kik provided IP address logins along with corresponding remote port numbers as well.

Kik also provided a text document entitled “bind” which is a log of about 8,230 IP addresses and corresponding remote port numbers that logged into the Kik account from February 17, 2021, through February 16, 2023. Investigators created a list of these IP addresses and determined the IP addresses that were used most often are 184.97.233.24, 184.97.226.51, 173.27.162.97, and 64.85.199.186. The IP address, 184.97.226.51 was also identified within the Kik conversation between Mason MOREY and Fun Forall on both December 4, 2022, and December 5, 2022.

36. A subpoena was sent to CenturyLink for subscriber data related to the IP address 184.97.233.24 and 184.97.226.51. CenturyLink responded with the following subscriber information (note: this is an excerpt of the full documentation that was returned to investigators).

Angela Hillen

2226 Tanner Bridge Road

Jefferson City, MO 65101

37. On or about April 6th, 2023, a subpoena was sent to MediaCom for subscriber data related to the IP address 173.27.162.97. MediaCom responded with the following subscriber information (note: this is an excerpt of the full documentation that was returned to investigators).

Vivian McKay

1310 Swifts HWY, Apt D205

Jefferson City, MO 65109

38. A subpoena was sent to Socket Telecom, LLC for subscriber information related to the IP address 64.85.199.186. Socket Telecom replied with the following subscriber information (note: this is an excerpt of the full documentation that was returned to investigators).

Equipment Share

Business Account

5710 Bull Run Drive

Columbia, MO 65201

39. On about February 27, 2023, a subpoena was sent to Google for subscriber data related to the email address fwbfunj@gmail.com. Google responded back with the following subscriber information (note: this is an excerpt of the full documentation that was returned to investigators).

40. GOOGLE SUBSCRIBER INFORMATION

Google Account ID: 1051030499993

Name: Brad Wilde

Given Name: Brad

Family Name: Wilde

e-Mail: fwbfunj@gmail.com

Alternate e-Mails:

Created on: 2014-11-24 23:50:49 Z

Terms of Service IP: 166.175.62.42

Services: Web & App Activity, Gmail, Google Calendar, YouTube, Google
Photos

Deletion IP:

End of Service Date:

Last Updated Date: 2021-08-22 07:51:33 Z

Last Logins:

ACCOUNT RECOVERY

Recovery e-Mail: Bmw01021970@hotmail.com

41. On March 23, 2023, a subpoena was sent to Hotmail for subscriber data related to email account Bmw01071970@hotmail.com. Hotmail returned the following subscriber data related to the aforementioned email address (note: this is an excerpt of the full documentation that was returned to investigators).

Query for: bmw01021970@hotmail.com

Date Range: Last Login Connection

Record Type (Registration) Registration Profile

Signin Name bmw01021970@hotmail.com

First Name B

Last Name Wilder

Region / State Missouri

Postal Code 65203

Country United States

Time Zone Indiana – EST

Creation Date and Time 4/23/2007 8:10:26 PM

Alternate Email

Record Type (IP Connection History) IP Connection History/Services Utilized

Last Modified Date and Time 3/9/2021 1:55:49 PM

Action Login Success

IP Address 107.77.208.141

Service Utilized Mail

42. Through an investigative search, Brian Matthew WILDER (DOB: 01/02/1970) was found to live in Jefferson City, MO at the address 2226 Tanner Bridge Road, Jefferson City, MO 65101. A Missouri driver license was also found for Brian WILDER. The photo on the driver's license for Brian WILDER showed a middle-aged white male subject with green/grey eyes, short grey hair, and a grey goatee. Employment records provided by HSI Springfield, MO showed WILDER's employer as "EquipmentShare.com INC" at 5710 Bull Run Drive, Columbia MO 65201. WILDER has been employed there from April of 2021 to the present.

43. A social media search was conducted as well and a Facebook page for Brian WILDER was found. WILDER's cover photograph was a picture of him, a white male subject appearing to be between the ages of 17-19 with blond hair, and a woman with brown hair. Facebook profiles were found for the two individuals in the photograph with WILDER.

The woman was identified as Angela Hillen and the younger male subject was identified as Camren Hillen.

44. WILDER's Facebook page also showed a woman named Vivian McKay listed as one of WILDER's friends. On Vivian McKay's Facebook page, she has Brian WILDER listed as her son within the family and relationships tab.

45. A search of the Angela Hillen's listed friends revealed a profile for Kris Wilder. A search of Kris Wilder's listed friends revealed a profile for Naomi Wilder. The profile picture for Naomi Wilder matched the female of picture 1a that Kik user Fun Forall sent to MOREY claiming to be a photograph of herself. Further review of other photographs in the Naomi Wilder profile revealed the exact same photograph that was sent to MOREY from Fun Forall. Naomi Wilder was identified as the wife of Seth Wilder, a relative of Brian WILDER.

46. A subpoena was sent to Facebook for subscriber information related to Brian WILDER's Facebook account. Facebook responded back with the following subscriber information (note: this is an excerpt of the full documentation that was returned to investigators).

Name:

First - Brian

Last – Wilder

Registered E-mail Addresses:

bmw01021970@hotmail.com, brian.wilder.50@facebook.com

Phone Numbers:

+15732917789 Cell Verified on 2020-01-12

47. Through an investigative search, a police report was found from the Cole County Sheriffs Office in Missouri. This report was conducted by a Deputy Officer who was investigating a sexual assault claim in March of 2012. A, then, 22-year-old male subject (henceforth referred to as MV1) explained he was the victim of a sexual assault. MV1 explained he has been communicating with someone who identifies as “Tricia” utilizing the email address fun4usall69@yahoo.com and phone number (573) 291-7789. “Tricia” and MV1 set up a time and place to meet on March 25, 2012. When MV1 arrived at the meet point, he sent a text to “Tricia” announcing his arrival. “Tricia” texted back explaining she was held up at work but will arrive shortly. While waiting for “Tricia” to arrive, MV1 fell asleep. MV1 was awoken by a male subject who identified himself as security for the area. The security guard was described by MV1 as a white male, about 6’2” - 6’3”, with short grey hair, and a few days growth of a beard. He also indicated that the man had crooked teeth. The security guard then told MV1 that he was going to call the police on him for trespassing unless MV1 were to “help him out”. MV1 saw the man had his penis out. MV1 stated he was going to call the police and the man responded, “who do you think they are going to believe, the guy who is trespassing or security?”
48. The report indicated that MV1 was noticeably upset while he spoke of the incident. MV1 stated that while he had the man’s penis in his mouth, he tried to pull away but the man grabbed his head and forced it back to his penis. The man pulled away and ejaculated on the ground. He then zipped up and left MV1. Through further investigative steps conducted by this Deputy, the phone number was identified as belonging to Angela

Hillen at 2226 Tanner Bridge Road, Jefferson City, MO. The Deputy found a Matthew Hillen and conducted a consensual interview with him.

49. Matthew explained that the phone number belongs to Brian WILDER, and he is the roommate of Angela Hillen. Matthew indicated that WILDER has lived with Angela Hillen for about 4 years.
50. The Deputy found the driver's license belonging to WILDER and showed the photograph to MV1. MV1 stated that it was hard to tell, but the photo looked very much like the security guard.
51. The Deputy found WILDER at 2226 Tanner Bridge Road and conducted a consensual interview. WILDER confirmed his phone number as (573) 291-7789 and his email as fun4usall69@yahoo.com. The deputy wrote in his report that he noticed the same crooked teeth, hair, and facial hair of WILDER matching the description of what MV1 gave. WILDER denied everything he was being accused of. Due to lack of physical evidence, nothing further happened with the case.
52. Columbia, Missouri Police received information that WILDER helps to care for his mother.
53. WILDER's mother has been determined to be Vivian McKay.
54. Cole County, Missouri property records indicate that the SUBJECT PREMESIS is owned by Vivian McKay but provide an alternate mailing address of 254 Blackhawk Drive, Lake Ozark, Missouri.
55. Camden County, Missouri property records indicate that Vivian McKay is still the owner of the address at 254 Blackhawk Drive, Lake Ozark, Missouri.

56. The SUBJECT PREMESIS is located in a condominium complex which is located immediately across the street from Helias Catholic High School and its associated athletic complexes in Jefferson City, Missouri.

57. The I.P. address associated with the SUBJECT PREMESIS used to access the Fun Forall Kik account accounted for approximately eight-hundred and four logins between November 2021 and February 2023. Access to the Kik account from the TARGET PREMESIS is approximately equal to the amount of access from I.P. addresses associated with WILDER's place of work and place of residence.

**CHARACTERISTICS OF INDIVIDUALS WHO RECEIVE AND COLLECT IMAGES
OF CHILD PORNOGRAPHY**

58. Based upon my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:

- a. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- b. Collectors of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual

arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

- c. Collectors of child pornography almost always possess and maintain their “hard copies” of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.
- d. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector’s residence, to enable the collector to view the collection, which is valued highly.
- e. Child pornography collectors also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- f. Collectors of child pornography prefer to have continuous access to their

collection of child pornography. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

59. Based upon the conduct of individuals involved in the collection of child pornography set forth above, namely, that they tend to maintain their collections at a secure, private location for long periods of time, there is probable cause to believe that evidence of the offenses of receiving and possessing child pornography is currently located at the premises described previously herein, known as, and the computers and computer media located therein.

SEIZURE OF EQUIPMENT AND DATA

60. Based upon my knowledge, training and experience, I know that in order to completely and accurately retrieve data maintained in computer hardware or on computer software, to ensure accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that some computer equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate such a computer, be seized and subsequently processed by a qualified computer specialist in a laboratory setting. This is true because of the following:

- a. The volume of evidence. Computer storage devices (such as hard disks, diskettes, tapes, laser disks, etc.) can store the equivalent of thousands of pages of information. Additionally, a user may seek to conceal criminal evidence by storing it in random order with deceptive file names. Searching authorities are thus required to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This sorting process may

take weeks or months, depending on the volume of data stored and it would be impractical to attempt this kind of data analysis on-site.

- b. Technical requirements. Analyzing computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know prior to the search which expert possesses sufficient specialized skills to best analyze the system and its data. No matter which system is used, however, data analysis protocols are exacting scientific procedures, designed to protect the integrity of the evidence and to recover even “hidden”, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (both from external sources or from destructive code imbedded in the system as a “booby trap”), a controlled environment is essential to its complete and accurate analysis.

61. Due to the volume of the data at issue and the technical requirements set forth above, it may be necessary that the above-referenced equipment, software, data, and related instructions be seized and subsequently processed by a qualified computer specialist in a laboratory setting. Under appropriate circumstances, some types of computer equipment can be more readily analyzed and pertinent data seized on-site, thus eliminating the need for its removal from the premises. One factor used in determining whether to analyze a computer on-site or to remove it from the premises is whether the computer constitutes an instrumentality of an offense and is thus

subject to immediate seizure as such-- or whether it serves as a mere repository for evidence of a criminal offense. Another determining factor is whether, as a repository for evidence, a particular device can be more readable, quickly, and thus less intrusively analyzed off site, with due consideration given to preserving the integrity of the evidence. This, in turn, is often dependent upon the amount of data and number of discrete files or file areas that must be analyzed, and this is frequently dependent upon the particular type of computer hardware involved. As a result, it is ordinarily impossible to appropriately analyze such material without removing it from the location where it is seized.

62. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - - for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to

retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

63. Based upon my knowledge, training, and experience, and the experience of other law enforcement personnel with whom I have spoken, I am aware that searches and seizures of evidence from computers taken from the subject premises commonly require agents to seize most or all of a computer system's input/output peripheral devices, in order for a qualified computer expert to accurately retrieve the system's data in a laboratory or other controlled environment. Therefore, in those instances where computers are removed from the subject premises, and in order to fully retrieve data from a computer system, investigators must seize all magnetic storage devices as well as the central processing units (CPU) and applicable keyboards and monitors which are an integral part of the processing unit. If, after inspecting the input/output devices, system software, and pertinent computer-related documentation it becomes apparent that these items are no longer necessary to retrieve and preserve the data evidence, such materials and/or equipment will be returned within a reasonable time.

64. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an

individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

COMPUTER EXAMINATION METHODOLOGY TO BE EMPLOYED

65. The examination procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other examination procedures may be used):

- a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying various file directories and the individual files they contain;

- d. opening files in order to determine their contents;
- e. scanning storage areas;
- f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or
- g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

BIOMETRIC ACCESS

66. Many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

67. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. The fingerprints authorized to access the particular device are a part of the security settings of the device and will allow access to the device in lieu of entering a numerical passcode or longer alphanumeric password, whichever the device is configured by the user to require. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the

bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

68. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. Apple's facial recognition feature is referred to as Face ID and it allows a user to unlock the iPhone X. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of the user's face. Face ID confirms attention by detecting the direction of the user's gaze, then uses neural networks for matching and anti-spoofing so the user can unlock the phone with a glance. Face ID automatically adapts to changes in the user's appearance, and carefully safeguards the privacy and security of the user's biometric data. Similarly, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes, and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

69. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within

the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

70. Beginning with the release of Apple's iOS 8 operating system in September 2014, Apple no longer has a key to decrypt these devices. Thus, even with a properly authorized search warrant to gain access to the content of an iOS device, there is no feasible way for the government to search the device.

71. Users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

72. As discussed in this Affidavit, there is reason to believe that one or more digital electronic devices, (Device(s)), will be found during the search. The passcode or password that would unlock any Device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

73. Biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch

ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Further, Touch ID will not allow access if the device has been turned off or restarted, if the device has received a remote lock command, or if five attempts to match a fingerprint have been unsuccessful. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.


74. A person who is in possession of a Device or has the Device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via biometric data, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device.

CONCLUSION

75. Based on the above information, there is probable cause to believe that the SUBJECT OFFENSES have been violated, and that the property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at the SUBJECT PREMISES described in Attachment A, and any computers, computer

media, or wireless telephones therein, and more fully described herein. Your Affiant requests authority to seize such material, specifically, that the Court issue a search warrant for these premises and all computers, computer hardware and media, and wireless telephones therein.

I state under the penalty of perjury that the foregoing is true and correct.



Mark Kutrip
Special Agent
Homeland Security Investigations

Attested to in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone or other reliable electronic means on April 21, 2023.



Willie J. Epps, Jr.
UNITED STATES MAGISTRATE JUDGE